

# 接入 Internet 的企业管控综合网络系统的设计

杨全胜 东南大学计算机科学与工程系 (210096)

## Abstract

This paper give a network configuration which has 3 layer, this configuration can ues in the integrative system which include autocontrol, MIS and link to Internet. In this paper, we discuss the system structure, the configure of hardware and software and the safety of this integrative system.

KeyWord: Internet, autocontrol, MIS

## 摘要

本文提出一种三层结构的具有接入 Internet 能力的企业管控综合网络系统。对系统总体结构, 软硬件配置以及安全问题进行了了探讨。

关键词: 国际互联网, 自动控制, 管理信息系统

## 1 概述

目前, 随着计算机尤其是网络技术的蓬勃发展, 很多企业都希望拥有自己的信息管理系统和生产监控系统相统一的网络系统, 将生产和管理直接挂钩, 形成了生产管理一体化的内部网络。特别是国家提出“企业上网计划”后, 各企业又面临着一个如何将内部网发布到国际互联网(Internet)上去的新的问题。

那么我们采用什么样的架构才能做到生产控制与管理直接挂钩, 尤其是连上 Internet 之后, 我们应该怎样在互联网上发布消息; 发布哪些消息; 以及如何处理由于连上互联网而带来的系统安全问题呢? 本文将从系统总体结构入手, 利用三层网络的模型, 并根据当前的实际情况给出一个切实可行的系统设计方案。

## 2 系统的总体结构

整个系统包括现场数据采集、控制, 工业生产的监测与监管, 生产性和非生产性数据管理以及有关数据的远程交付和企业信息的国际互联网发布等诸多内容。所有这些内容如果都建立在一个单独的企业内部网络上, 显然是很复杂, 也是很很不安全的。

在我们研制的 SE-DCS 系统中, 采用了三层网络结构, 如图所示: 现场网络可以是象 485 这样的总线构造的主从式网络。网络中从机是各种型号的智能采集监控设备(智能采集监控站), 主机是作为上位机的 PC 机。这一层网络在工业控制现场, 负责现

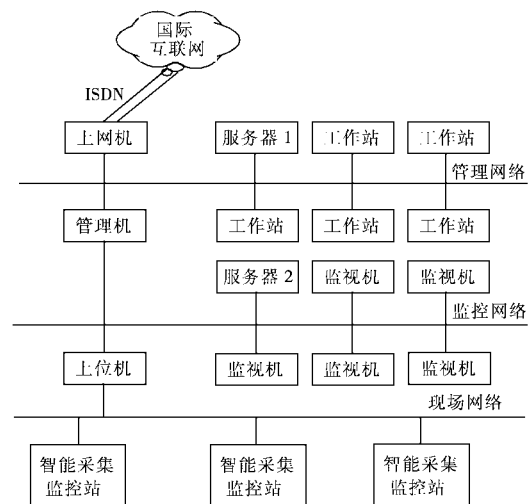


图 网络结构图

场的数据采集和控制。

监控网络采用 Windows NT 作为服务器, 这是现场操作工人的使用平台, 包括一个服务器, 一个现场网络的上位机和若干台作为操作工平台的监视机, 操作工人可以利用这个平台获取现场信息以及控制现场的操作, 同时, 生产管理员可以在这一层网络上对该层网络和现场层网络的各个部件进行初始化。

管理网络包括企业中生产性和非生产性的数据的管理, 也就是我们常说的 MIS 管理系统的功能, 但对于要接入到 Internet 网络的系统, 在这一层要作好上网的准备和设置。同时从服务器 2 中获取生产数

据,将必要的部分转换到供上网使用的服务器 1 中。

这样的三层结构将控制现场、操作现场和后台管理以及 Internet 隔离开来,一方面,各个层次可以单独设计,单独运行,简化了设计时期的复杂性,其次,由于不同的部门分属不同的网络,也保证了各个部分数据的相对安全性。

### 3 各功能模块的基本功能描述

智能采集监控站直接和前端的传感器和控制部件相连,它们带有自己的微处理器, A/D、D/A 转换部件以及一定容量的存储器,能自行进行数据采集,报警记录,同时,通过 485 总线,和上位机相连。

上位机主要有三大功能:第一,作为现场网络的上位机,整体负责现场网络的运转,现场网络中的各种智能采集设备的添加、更换,初始化等工作都由上位机负责,同时,该机器还负责现场网络的通信管理,所有智能采集监控站之间的数据流通由上位机实现。第二,上位机作为监控网络的数据源机器。它将从现场网络的各个数据采集站得到的数据送到数据库 2 中,并同时在现场网络中进行广播。第三,对监控网络的各个监视机的组态软件进行实时功能和数据的组态,搭构新的执行软件。

监视机上有可组态的现场监控软件,提供操作人员监视现场和控制现场的功能。如果需要更改智能采集监控站,可以利用组态软件进行及时修改和下载。

服务器 2 作为监控网络的服务器,负责记录上位机从现场网络中得到的实时数据和经过计算后的生产报表数据。供监视机和管理机进行查询和使用。

服务器 1 作为管理网的服务器,负责记录各种非生产数据,包括人事、材料、财会等数据以及从服务器 2 中获得的部分生产数据。

管理机介于管理网络和监控网络之间。它的主要任务是将监控网络服务器 2 中的实时生产数据根据管理网络的需要进行转变,并定时传送到服务器 1 中。

工作站是供各行政和执能部门使用的,它们可以遍布企业的各个部门。

上网机是整个系统和 Internet 网的接口,通过它向国际互联网发布信息,以及从国际互联网获得有用的信息。

应该指出的是各个部件之间既是独立运转的,又是紧密联系的。比如,各个智能采集监控站可以单独采集和控制某些信号和开关,同时,在上位机的统一

指挥下,又合作完成更大的控制任务,以及在有事件到来的时候,联合加快对某些相关测点的加速采样;各监视机既是本岗位的数据监视与控制平台,在上位机的实时组态下,它也可以配合其它班组进行协同监控。

## 4 各层网络的系统软硬件配置

### 4.1 现场网络层

我们采用了智能采集控制前端(如国内使用广泛的 893),该类智能控制前端利用 485 总线彼此相连,并使用该总线和上位微机相连接,为了保证可靠,我们使用了两个上位机,互为备份。智能采集控制前端直接和具体的执行部件和传感器相连接,放在尽可能靠近测控点的现场,能保证易受干扰的小信号的传输尽可能短。

上位机使用 Windows 95 平台,自行编写了初始化各种采集控制前端的软件,以及可组态的采集模块和报表实时生成模块,随时测得数据,随时就能更改报表中的相关的值。

### 4.2 监控网络层

由于该层具有很强的实时性,又需数据库的支持,所以我们在本层采用 Windows NT 服务器,同时采用 SQL Server 作为数据库。除服务器外,其它各种机器均使用 PC 机。开发软件采用了 Visual C++。

上位机在这一层中将实时数据利用网络广播功能发送到各个监视机,并按照各种统计要求,迅速计算出各项报表的数据和统计数据,保存到数据库中。

监视机配备了自行开发的可组态监控软件(也可以配备象“组态王”那样的商业软件)。除了实时显示各测试点的数据外,还可做控制平台、查看历史数据与有关报表的平台。

### 4.3 管理网络

考虑到和 Internet 接轨,所以,在这一层,我们没有采用传统的 Foxpro, 或者 Access 开发软件做开发,而是将这一层建成了一个企业内部的 Intranet。

服务器上采用了 Windows NT + IIS + SQL Server 的架构,实际上构成了一个能支持互联网上的站点服务器。但考虑到安全问题,这个服务器并没有对外公开。

其它的各种工作站一般采用 Web 浏览的办法来访问服务器上的数据库。数据库的维护,主页的制作由专人负责,其中生产报表的数据直接由管理机从服务器 2 中产生并自动转换和保存到服务器 1 中。采用 web 浏览方式,当需要增加或修改工作站上的软件,

用户可以直接编写有关的html主页,非常灵活,不受开发软件的限制。但是,它要求用户需要掌握ASP, JSP, 主页制作等多种技能,一般企业可能难以承担,所以,我们在这里,还是对部分技术难度较高的功能使用了常规编程方法编写软件,供用户使用。

为了用户能很好地运用Web浏览技术开发新的界面和功能,以及将本企业的信息发布到国际互联网上,在本层提供了相关的开发工具,如InterDev, Frontpage等等。本层的这种软件环境的安排,顺应了当前e时代的发展。

同时,利用ISDN将该层网络的部分机器连到国际互联网上。

## 5 系统安全性分析

从整体结构上可以看到,该系统上通国际互联网,下通工业生产的直接现场,系统跨度大,设计的部门多,设计的技术也很多,必然会带来更多的安全隐患。一般来说,我们认为该系统存在的安全隐患来自于上中下三个方面。

来自下面的安全隐患主要是从现场过来的各种干扰信号,由于工业现场环境复杂,粉尘、腐蚀性物质、潮湿、电磁波、震动、温度等各种因素都会对硬件和软件带来影响;来自中间层的安全隐患大多来自于操作人员的操作失误和软件的错误,归结起来就是软件的健壮性问题;来自上面的安全隐患是由于系统接入Internet之后,从国际互联网上到来的新的安全问题,比如黑客入侵造成的数据失密或丢失,更严重的可能造成系统的瘫痪。分析清楚安全隐患的来源,对我们指定安全措施很有帮助,下面是SE-DCS采用的安全措施。

首先是分层的总体结构,使得整个系统被分成了三个部分,我们有意没有将服务器跨接到两个网络之中,而是在每两个网络中采用工作站(管理机和上位机)来跨接,这样,使得服务器受到破坏的机会变小。另外由于分出了层次,所以任何问题一般都只能影响到本层网络,不会影响整个系统。

对于下层来的安全隐患,采用达到国际安全级别的只能采集控制设备是很关键的,因为他们能很有效地防止分层、腐蚀性物质、潮湿的侵害;好的光电隔离能比较好地解决电磁干扰问题。最为重要的是前端采用集散型采集监控系统,利用分散采集和控制,集中管理的办法,使来自下层的干扰的影响面尽可能缩小,而且一个智能采集监控设备是损坏不会影响整个现场网络层。由于是集散型设计,也使得各个单元的

功能相对简单,而简单的同时,也带来了高的可靠性;在软件方面,要对得到的各种数据进行合理性判断,确保错误数据不通过上位机传到上一层网络中。

对于来自中层的不安全因素的排除在很多程序设计的课程中都已经讲述过,本文不展开讨论。

来自上层的安全问题是近年来随着互联网的发展而带来的,值得我们关注。在这个层次上我们主要要防范的是来自计算机病毒的侵犯和来自网络上的黑客的侵犯。装备相应的防火墙是一个不错的方案,病毒防火墙有很多种,比较著名的有瑞星, KILL, PC-cillin, VRV等等。对于网络上的安全可以分成两步,网络信息发布用的服务器,可以采用租用空间的办法,这样,服务器安全会有专门的技术人员负责,也可以利用服务器托管(当需要容量比较大的时候),这种办法可以培训专门的技术人员负责服务器安全,并在服务器上加装服务器型的防火墙。一般来说,企业上网的一个目的是在网上介绍本企业的产品,所以租用一定容量的服务器空间是一个即安全又方便的办法。企业上网的另一个目的是为了获得国际互联网上的相关资料,这样,必然需要企业内部分机器能上互联网,而这些机器一旦被入侵,很可能波及整个管理网络,因此这些机器上,应该全部加装个人网络防火墙,比较著名的个人防火墙有LockDown、Conseal PC Firewall等。这些防火墙可以有效地阻止恶意入侵和木马程序的隐藏。

## 6 总结

本文提出的三层网络结构的具有接入Internet能力的企业管控综合网络系统,顺应了当前企业上网的要求,又符合企业自动控制生产和科学管理信息的要求,它比单网结构更容易设计,更安全,也更为合理。适合于中小型企业自动化生产管理应用,同时由于具有Internet接入功能,利用这个接口,也能实现大型集团综合管理各分厂的应用。

## 参考文献

1. 王常力 廖道文主编,“集散型控制系统的设计与应用”,清华大学出版社,1993
2. 杨全胜,“集散监测与信息管理一体化系统的设计与实现”,计算机系统应用,1994. 12
3. 杨全胜,“开放式集散监控系统的设计与实现”,气象仪器装备,1996. 1
4. 深蓝,ISDN简介,计算机应用文摘,2000 增刊
5. 杨守君,黑客技术与网络安全,中国对外翻译出版公司,2000